

**Department of Homeland Security
Information Analysis and Infrastructure
Protection
Daily Open Source Infrastructure Report
for 05 June 2003**

Current Nationwide
Threat Level is



[For info click here](http://www.whitehouse.gov/homeland)
www.whitehouse.gov/homeland

Daily Overview

- The Washington Post reports the Transportation Security Administration disclosed Tuesday that it fired 1,208 screeners at airports nationwide, including 85 convicted felons, after discovering that the workers had questionable backgrounds. (See item [6](#))
- The Washington Post reports a state-by-state analysis released Tuesday concludes the nation's public health laboratories are dangerously unprepared for a chemical attack. (See item [13](#))
- Microsoft has released "Security Bulletin MS03-020: Cumulative Patch for Internet Explorer (Critical)" which includes the functionality of all previously released patches for Internet Explorer 5.01, 5.5 and 6.0, and eliminates two vulnerabilities. (See item [17](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *June 03, Reuters* — **Mirant bankruptcy threat shakes U.S. energy market. Rumbblings from electricity generator Mirant Corp. that it might seek bankruptcy protection have stirred nerves in an already troubled energy market**, traders said on Tuesday. "Mirant is a big company that could potentially disrupt the market. They are probably holding a lot of positions," one Midwest natural gas trader said. **Atlanta-based Mirant, one of the nation's top merchant energy traders, on Monday offered its creditors a plan to restructure \$1.45 billion of debt as part of a wider refinancing effort aimed at avoiding bankruptcy.** At the same time it warned that if the plan were not quickly approved, it might seek Chapter 11

bankruptcy protection using the same plan as the foundation for restructuring. The move is the latest in a series of setbacks for an industry hit hard by the downfall of energy trader Enron Corp. in 2001, federal investigations into market manipulation and subsequent severe credit downgrades. "Mirant is one of the few big players left," one New England electricity trader said. "If Mirant exits the market, it's going to be a lot harder to enter long term deals." **A year ago, Mirant was the biggest natural gas trader and sixth biggest power trader in the United States**, according to a study by energy analyst Scott, Madden & Associates. Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3887439

2. *June 03, PR Newswire* — **Pennsylvania Governor Rendell announces changes in deployment at nuclear power plants. Pennsylvania Governor Edward G. Rendell today announced that the Pennsylvania National Guard will conclude its around-the-clock deployment at each of the state's five nuclear power plants on Wednesday, June 4.** The 24-hour presence has been in effect since Friday, May 23, when the federal and state terrorist threat level was raised to Orange (High). On Friday, May 30, the federal and state terrorist threat level was lowered to Yellow (Elevated). **Governor Rendell said the National Guard and the Pennsylvania State Police will continue to provide random, unannounced patrols at the nuclear power plants.** Governor Rendell made the decision after consulting with members of his Homeland Security Team, including Pennsylvania State Police Commissioner Col. Jeffrey Miller, Adjutant General William Lynch, Pennsylvania Emergency Management Agency Director David Sanko and Office of Homeland Security Director Keith Martin. **"Given the recent decrease in the terrorist threat level and the fact that there continues to be no credible threat against any nuclear power facility in Pennsylvania or the United States, my Homeland Security Team has recommended that the around-the-clock deployment be modified,"** Governor Rendell said.

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=comtex_2003_06_03_pr_0000-3067-pa-pema-deplo_ymenta

3. *June 03, Associated Press* — **Czech nuclear plant unit shut down following steam leak. A minor steam leak forced workers to shut down a reactor at a nuclear plant near the Austrian border, a spokesman said Tuesday. No radioactivity was released.** Milan Nebesar, spokesman for the Temelin nuclear plant, said the reactor was shut down early Tuesday after workers detected a minor steam leak in the unit's non-nuclear section. The unit was expected to be reconnected to the power grid on Wednesday. The plant's second reactor continued to run at full capacity, Nebesar said. The plant's two 1,000-megawatt units are undergoing final trials required before they start commercial power generation. The unit temporarily shut down Tuesday is expected to be ready for commercial use sometime this year. It began an 18-month full-scale test run in June 2002. The second unit is expected to be ready for commercial use in 2004. **The Temelin plant, based on Russian design and upgraded with U.S. technology, has been plagued by frequent non-nuclear malfunctions since testing began in November 2000. Located just 60 kilometers (35 miles) north of the Austrian border, it has been a source of friction between the two countries. Critics in Austria argue the plant is unsafe and have repeatedly demanded that it be shut down, but Czech authorities insist the plant is safe.**

Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3887976

Chemical Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

4. *June 04, Washington Post* — **Air defense to be tested Wednesday night over Washington, DC.** The drill will start at 10:30 p.m., and involves two F-16s that will intercept two Cessna 172 civilian airplanes in a scenario designed to test pilots, antiaircraft missile crews and civilian and military commanders. A spokesman said the jets will take off from Andrews Air Force Base but declined to provide further details on the affected airspace. He said that the exercise was scheduled for the period when civilian air traffic is lowest and that flight paths were adjusted to reduce the noise level. **"We've changed some of the flight profiles to minimize the noise as much as possible, but people still will be able to hear some of these things,"** said Major Don Arias, a spokesman for the North American Aerospace Defense Command (NORAD). **He added that the F-16s would not use afterburners below a certain altitude.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A10185-2003Jun 3.html>

5. *June 04, U.S. Department of Defense* — **National Guard and Reserve mobilized as of June 4, 2003. This week the Army, Navy, Air Force and Marine Corps each announce a decrease of reservists on active duty in support of the partial mobilization. The net collective result is 4,521 fewer reservists than last week.** At any given time, services may mobilize some units and individuals while demobilizing others, making it possible for these figures to either increase or decrease. Total number currently on active duty in support of the partial mobilization for the Army National Guard and Army Reserve is 142,364; Naval Reserve 11,335; Air National Guard and Air Force Reserve, 35,970; Marine Corps Reserve, 21,197; and the Coast Guard Reserve, 4,305. **This brings the total Reserve and National Guard on active duty to 215,171 including both units and individual augmentees.**

Source: <http://www.defenselink.mil/releases/2003/nr20030604-0078.htm>

[\[Return to top\]](#)

Banking and Finance Sector

Nothing to report.

[\[Return to top\]](#)

Transportation Sector

6. *June 04, Washington Post* — **1,208 airport workers fired after checks. The Transportation Security Administration (TSA) disclosed Tuesday that it fired 1,208 screeners at airports nationwide, including 85 convicted felons, after discovering that the workers had**

questionable backgrounds. The number included 503 screeners who failed to notify the agency that they had been arrested or convicted of a crime. The agency that oversees airport security discovered the workers' disqualifications in recent months as it finishes vetting screeners already on the job. TSA head James M. Loy suggested that a troubled contract with a company in charge of recruiting and assessing applicants for airport screening jobs might be partly to blame for the incomplete background checks. **Loy pledged to lawmakers that a thorough check would be completed by October 1. But he also took responsibility for the problems and said the nation should have confidence in airport security personnel.** The TSA was charged with hiring tens of thousands of airport screeners in a mad rush last fall to fulfill a congressional mandate after the September 11, 2001, terrorist attacks. Congress set standards to create a more skilled, educated and highly paid federal workforce of airport screeners that had to pass more thorough background checks.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A9877-2003Jun3.html>

7. *June 04, CNN* — **Spanish trains collide head-on. At least 19 people were killed and 40 others injured when a passenger train collided head-on with a cargo train in southeastern Spain,** the state rail company said Wednesday. Rescuers are searching for eight people still unaccounted for after two leading cars of the passenger train were destroyed in the crash and ensuing fire, CNN's Spanish partner station CNN+ reported. **Spanish Development Minister Francisco Alvarez-Cascos said the cause of the crash may have been a railway worker who gave a wrong signal,** the Associated Press reported. The passenger train was carrying about 90 people, while the 28-car freight train had two crew members on board, AP said. The crash occurred late Tuesday near the village of Chinchilla, in the Spanish province of Albacete. **Spain's largest newspaper, El Pais, reported on its Web site that the cargo train carried at least some empty containers that previously had transported chemical products.**

Source: <http://www.cnn.com/2003/WORLD/europe/06/04/spain.trains/index.html>

8. *June 03, Washington Post* — **U.S. Coast Guard defends security efforts.** The commandant of the U.S. Coast Guard parried lawmakers from both parties who accused the Bush administration Tuesday of moving too slowly to secure the nation's ports against terrorism. **Adm. Thomas H. Collins acknowledged that the Coast Guard still needs an additional \$70 million and 150 full-time employees by this fall to implement a broad new maritime security law enacted after the attacks of September 11, 2001.** But Collins said he is confident the administration recognizes the threat and will come through with the money. **The panel's chairman wasn't convinced. Rep. Frank LoBiondo (R-NJ), said he was distressed to learn the administration may cover cost overruns in airport security by shifting money designated for port security grants.** Transportation Secretary Norman Mineta said last week that he considers America's ports to be the most vulnerable segment of the transportation industry today. Collins said the Coast Guard will release interim rules next month to implement the maritime security law Bush signed in November.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A8605-2003Jun3.html>

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

Agriculture Sector

9. *June 03, Associated Press* — **Canada to slaughter, test more cattle. Canadian authorities ordered the destruction and testing of 650 more cattle for mad cow disease because DNA testing failed to confirm the origin of the lone cow known to be infected so far, an investigator said Tuesday.** The animals from five Alberta farms will be killed and have samples of their brains checked in laboratories, said Brian Evans, chief veterinary officer of the Canadian Food Inspection Agency. **The new tests will likely delay by several days the conclusion of the investigation into any possible spread of bovine spongiform encephalopathy, or BSE.** Evans had said Monday the investigation could be finished by the end of the week. That is bad news for the Canadian beef industry, which wants the United States and other countries to lift bans on Canadian beef imports as soon as possible. **Sales and production have slowed since the bans began as far back as May 20, and industry figures say the impact increases each day that product cannot be moved.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A9776-2003Jun3.html>

Food Sector

10. *June 04, Education Week* — **Tainted food on the rise in cafeterias. Outbreaks of food-borne illness are on the rise in U.S. schools, increasing by 10 percent a year in the 1990's, even as recent federal health data show a significant decrease in food poisoning in the general population.** Reports in recent years suggest the blame for that disparity can't be easily assigned to any one public or private entity. **Food poisonings in schools have been traced to poor hygiene in processing plants, improper storage and heating of food in school kitchens, and even the unwashed hands of students. But in 59 of the largest outbreaks of such illnesses in schools from 1990 through 1999, roughly two-thirds, or 40 incidents, were traced to food provided through the federal school meal programs, according to a U.S. General Accounting Office report scheduled for release this week.** Those meals, served to 28 million children daily, are ultimately the responsibility of the U.S. Department of Agriculture.

Source: <http://www.edweek.org/ew/ewstory.cfm?slug=39food.h22>

11. *June 04, Reuters* — **USDA issues new rules to prevent listeria in meat. The U.S. Agriculture Department (USDA) on Wednesday announced new rules for meat plants to help keep potentially deadly listeria bacteria from hot dogs, deli meats, and sausage. The new USDA rule requires U.S. meat plants that produce ready-to-eat products exposed to the environment after cooking to develop a plan to prevent listeria, then to verify the effectiveness of the plan through testing.** "This rule is tough; it's fair; it's based on science," said Elsa Murano, USDA undersecretary for food safety. "It will require plants to share their testing data." About 2,500 U.S. meat plants produce ready-to-eat meat products, which do not have to be cooked by consumers.

Source: <http://reuters.com/newsArticle.jhtml?type=politicsNewsID=2878318>

[\[Return to top\]](#)

Water Sector

12. *June 04, Reuters* — **UN nuclear agency tries to avert water crisis. The International Atomic Energy Agency (IAEA) is showing countries how to tap the world's many underground springs.** "The management of water resources is the most important thing for water scarcity, because you have to know where it is and how much is there in order to minimize or avoid water shortages," said Pradeep Aggarwal, head of the IAEA's isotope hydrology department. Isotope hydrology is not a new science and has been around as long as nuclear science. **But the IAEA, which has helped some 45 countries set up isotope hydrology labs, says the simple and relatively cheap technique is still not used widely enough.** The idea is simple. Water contains natural isotopes, which are atoms of the same element but with different atomic weights. So-called heavy water contains more heavier isotopes. **By tracking these isotopes, which give the water source its "fingerprint", water engineers can quickly obtain information that would normally require half a century of measuring rain, river and water body levels.**

Source: <http://www.planetark.org/dailynewsstory.cfm/newsid/21011/story.htm>

[\[Return to top\]](#)

Public Health Sector

13. *June 04, Washington Post* — **Readiness for chemical attack criticized. The nation's public health laboratories are "dangerously unprepared" for a chemical attack, according to a state-by-state analysis released Tuesday. The vast majority of labs do not have the equipment or expertise to identify a wide range of potential chemical weapons, including ricin, cyanide, sarin, VX, and most pesticides, the nonprofit, Trust for America's Health reported.** Nearly 18 months ago, the Department of Health and Human Services identified chemical testing as one of seven priorities for state health departments. But little progress has been made, officials concede, in large measure because bioterrorism projects overshadowed all over preparedness work. **Not a single state lab has the capability to test for many of the most common chemicals, such as phosgene, a poison that can cause severe lung damage, and arsine, a gas that when inhaled can lead to permanent organ damage and death. Only two states have the equipment and expertise to test for cyanide, although the highly toxic compound is commercially available or naturally found in 41 states. Only eight states have drafted plans for responding to a chemical attack.** "We know we need to develop this capacity," said Joseph Henderson, associate director for bioterrorism at the U.S. Centers for Disease Control and Prevention (CDC). " He said that the proper lab equipment is expensive and that chemical testing requires extensive training. **This year, the CDC intends to allow states to use portions of their federal grants for chemical lab expansion if they choose.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A9900-2003Jun3.html>

[\[Return to top\]](#)

Government Sector

14. *June 04, U.S. Department of Justice* — **Interim report: development of the national criminal intelligence sharing plan.** This interim report presents the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) preliminary recommendations for achieving the goals and objectives outlined in the International Association of Chiefs of Police (ICAP) Criminal Intelligence Sharing Report. These recommendations are also in response to direction from the Bureau of Justice Assistance (BJA), the Global Advisory Committee (GAC), and the IACP for development of a National Criminal Intelligence Sharing Plan. The August 2002 IACP Criminal Intelligence Sharing Report contained a proposal to create a national Criminal Intelligence Sharing Plan. **The most central and enduring element was the recommendation for the creation of a Criminal Intelligence Coordinating Council comprised of local, state, tribal, and federal law enforcement executives. The Council's mandate would be to establish, promote, and ensure effective intelligence sharing and to address and solve, in an ongoing fashion, the problems that inhibit it.** In fall 2002, in response to this proposal, the U.S. Department of Justice, Office of Justice Programs (OJP), BJA, authorized the formation of the GIWG.

Source: <http://www.it.ojp.gov/documents/intellplan.pdf>

15. *June 04, Philadelphia Inquirer* — **Constitutional change is urged in case terror strikes Congress.** The Constitution must be amended to ensure the continuity of government in case Congress is wiped out by a terrorist attack, a blue-ribbon bipartisan commission will recommend on Wednesday. **If a September 11-like attack destroyed Congress, the current system of holding special elections to fill vacancies in the House of Representatives would take too long – an average of four months, depending on the state – the panel found after a yearlong study. Governors currently fill U.S. Senate vacancies, but without an amendment allowing similar temporary appointments to the House until elections could be held, the nation could have no functioning Congress in a time of great crisis.** "In the event of a disaster that debilitated Congress, the vacuum could be filled by unilateral executive action – perhaps a benign form of martial law," the commission found. "The country might get by, but at a terrible cost to our democratic institutions." The 15-member bipartisan panel was chaired by veteran presidential adviser Lloyd Cutler, a Democrat, and former Sen. Alan Simpson of Wyoming, a Republican.

Source: <http://www.philly.com/mld/inquirer/news/nation/6007104.htm>

16. *June 04, Contra Costa Times* — **Local labs form partnerships for security's sake.** The national laboratories are hot on the trail of homeland security research, but they can't do it alone, a top official from the Department of Homeland Security said Tuesday. **They need to partner with companies to quickly turn technologies into reality for firefighters, police officers and other emergency officials, said Mike Burns, head of the department's Office of National Laboratories. Equally important, the labs must do a balancing act of working together to coordinate and evaluate research, while competing also in the world of ideas.** "Homeland security is an enduring mission," said Burns, who was in the Bay Area for a meeting of lab officials who work to transfer technology from scientists to companies. "Many national labs have understood that and have stepped up to the plate."

Source: <http://www.bayarea.com/mld/cctimes/6009892.htm>

[\[Return to top\]](#)

Emergency Services Sector

Nothing to report.

[\[Return to top\]](#)

Information and Telecommunications Sector

17. *June 04, Microsoft* — **Microsoft Security Bulletin MS03–020: Cumulative Patch for Internet Explorer.** This cumulative patch includes the functionality of all previously released patches for Internet Explorer 5.01, 5.5 and 6.0, and eliminates two vulnerabilities: **a buffer overrun vulnerability that occurs because Internet Explorer does not properly determine an object type returned from a web server, and a flaw that results because Internet Explorer does not implement an appropriate block on a file download dialog box.** It could be possible for an attacker to exploit this vulnerability to run arbitrary code on a user's system. This cumulative patch will cause window.showHelp() to cease to function if you have not applied the HTML Help update. **Microsoft has assigned a risk rating of "Critical" to this patch.**

Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03–020.asp>

18. *June 04, Post Newsweek Tech Media* — **PKI momentum builds, program manager says.** A dozen years after the start of the federal push for a public–key infrastructure, the technology is gaining momentum, and more agencies will be using PKI in a matter of months, a federal program manager predicts. **By year's end, Tim Polk, the PKI program manager at the National Institute of Standards and Technology, estimated, eight to 10 agencies will be heavily engaged in PKI,** nearly twice the number involved today. Polk spoke today at a conference on IT security in Washington sponsored by the research and advisory firm Gartner Inc. As governments and businesses move from paper to electronic documents, **PKI holds promise as an effective way to protect and validate those documents and verify identities. PKI also is being used with employee identification smart cards.**

Source: http://www.gcn.com/vol1_no1/daily–updates/22320–1.html

19. *June 03, National Journal* — **Computer security officials discount chances of 'digital Pearl Harbor'.** The notion that the cyberterrorism against the United States could create a "digital Pearl Harbor" is fading three computer–security experts said Tuesday. Casey Dunlevy of Carnegie Mellon's Software Engineering Institute (SEI), and Richard Hunter of Gartner Group, said **disgruntled insiders, not foreign terrorists, pose the greatest cybersecurity threat to companies.** "But could [cyber terrorism] be a force multiplier in terrorist attacks" by, for example, disabling all traffic lights after a bombing? "I think we have to consider that," said Dunlevy. He said **computers recovered from Afghanistan demonstrated al Qaeda's use of steganography, a technique for embedding secret data within pictures or text.** "We will eventually see a cyber element to terrorist activity," Dunlevy said. But both he and Hunter said **terrorist groups also are likely to continue to**

engage in money laundering and cybercrime as a means of purloining resources.

Source: <http://www.govexec.com/dailyfed/0603/060303td2.htm>

20. June 02, Federal Computer Week — Rural region models safety system. The Virginia Department of Transportation, several private-sector health and nonprofit groups and a number of jurisdictions in the valley are developing an integrated, Web-based communications platform for first responders. Led by the Northern Shenandoah Valley (NSV) Steering Committee, the initiative began three years ago as an effort to improve highway safety and the response to crashes and hazardous material spills along the state's Interstate 81 corridor. But after September 11, 2001, there was a "pretty significant sea change" in the project's scope, said Jack Potter, chairman of the NSV committee. The steering committee began refining the Integrated Intelligent Transportation System – Public Safety System during the past year. **The system automatically collects and aggregates data for future analysis, can act as a disease surveillance system, and even provides specific information about certain patients whom paramedics frequently treat.**

Source: <http://www.fcw.com/geb/articles/2003/0602/web-nsv-06-02-03.a.sp>

Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: WORM_LOVGATE.G Source: http://wtc.trendmicro.com/wtc/wmap.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios-ns), 80 (www), 1434 (ms-sql-m), 445 (microsoft-ds), 113 (ident), 139 (netbios-ssn), 0 (----), 53 (domain), 4662 (eDonkey2000), 25 (smtp) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

[\[Return to top\]](#)

General Sector

21. June 04, New York Times — U.S. security backlog strands many refugees in camps abroad. More than 20,000 refugees approved for resettlement in the United States remain stranded in desolate camps in Africa, Asia and the Middle East as officials here continue to struggle to reduce the backlog of required security clearances, State Department officials say. **The officials say they are working to speed up the process. About 14,300 refugees were admitted during the first eight months of the current fiscal year, up from nearly 3,000 during the**

corresponding months of the last fiscal year, which was disrupted by the terrorist attacks of September 11, 2001. But the officials say refugee admissions are still far below normal. In recent years, about 42,000 refugees have been resettled during the first eight months of the fiscal year. The government had hoped to resettle 50,000 refugees by September 30, the end of the fiscal year, but that seems unlikely.

Source: <http://www.nytimes.com/2003/06/04/international/04REFU.html>

22. *June 04, Wired* — **Smartcams take aim at terrorists. The Department of Defense awarded \$600,000 to University of California at San Diego's Computer Vision and Robotics Research (CVRR) lab Friday for further development of distributed digital video arrays (DIVAs), cameras that see, think and communicate.** Granted through a federal counterterrorism interagency task force called the Technical Support Working Group, **the funding is slated to help CVRR redirect these intelligent camera systems from their initial intent, which was preventing traffic delays, to stopping terrorism.** For the past four years, CVRR's DIVAs assessed traffic patterns, located accidents and notified firefighters of emergencies, according to Mohan Trivedi, director of the DIVA project. Even with the advent of the Department of Homeland Security and orange security alerts, **round-the-clock guards have never been feasible for every national landmark or "important location." But cameras, installed and mobile, just may be.**

Source: <http://www.wired.com/news/technology/0,1282,59092,00.html>

23. *May 29, Homeland Security & Defense* — **Universities forming alliances to seek funding for homeland security research.** Corporate America isn't the only sector trying to get a piece of the homeland security funding pie. **Universities around the country also are forming partnerships and alliances to win federal research funds.** On New York's Long Island, Stony Brook University is joining with defense contractors, researchers and high-tech companies to lobby Washington for homeland security research money. In New Mexico, two universities have teamed up to buy a small, largely abandoned, copper smelting town and turn it into a national training and research center for emergency responders and bio-security. **From new courses of study to new emergency preparedness centers, institutions of higher learning across the country are looking to connect to the issue of home land security.**

Source: http://www.aviationnow.com/avnow/news/channel_hsd_story.jsp?id=news/research05293.xml

[[Return to top](#)]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Warnings](#) – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Publications](#) – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 202-324-1129

Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202-323-3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.